
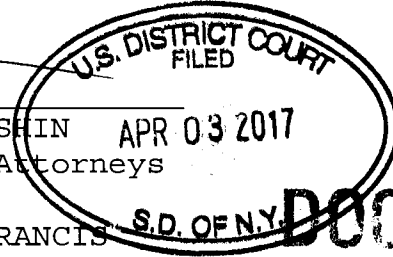


ORIGINAL

Approved: EUN YOUNG CHOI / WON S. SHIN
Assistant United States AttorneysBefore: THE HONORABLE JAMES C. FRANCIS
United States Magistrate Judge
Southern District of New York

17 Mag. 2467

UNITED STATES OF AMERICA

- v. -

ZHENGQUAN ZHANG,
a/k/a "Zheng Quan Zhang,"
a/k/a "Jim Z. Zhang,"

Defendant.

SEALED AMENDED COMPLAINTViolations of
18 U.S.C. §§ 1832 and 2COUNTY OF OFFENSE:
NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

MICHAEL DENICOLA, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation (the "FBI"), and charges as follows:

COUNT ONE
(Theft of Trade Secrets)

1. From at least in or about December 2016 through in or about March 2017, in the Southern District of New York and elsewhere, ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang," the defendant, with the intent to convert a trade secret that is related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of others than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, knowingly did steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice and deception obtain such information; and without authorization did copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information; and attempted to do so, to wit, ZHANG stole and attempted to convert to his own use the computer source code

underlying proprietary trading software, which was a trade secret of a financial services company for which ZHANG worked.

(Title 18, United States Code, Sections 1832 and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

2. I am a Special Agent with the FBI, and I have been personally involved in the investigation of this matter. I have been a Special Agent with the FBI since approximately June 2015. Since becoming a Special Agent with the FBI, I have been assigned to a computer intrusion squad in the FBI's New York Field Office. In that role, I have participated in numerous investigations of computer crimes, among other federal crimes. This affidavit is based upon my own observations, conversations with witnesses, and conversations with other law enforcement agents, as well as on my examination of reports and records prepared by others. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all of the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. In the course of this investigation, I have spoken to representatives of a financial firm engaged in the trading of a variety of publicly traded securities and other financial products ("Firm-1") and reviewed publicly available documents and records. Based on those conversations and that review, I am aware of the following information, in substance and in part, regarding the operations of Firm-1:

a. Firm-1 acts as a market maker, facilitating trading and liquidity in a variety of financial markets. Firm-1 engages in billions of dollars of equities and fixed income trading on a daily basis.

b. Firm-1 is headquartered in New York, New York and maintains offices and other facilities in various locations in the United States and abroad, including but not limited to an office in San Jose, California and a data center

in Purchase, New York. The majority of Firm-1's employees are located at Firm-1's New York headquarters.

4. In the course of this investigation, I have spoken to representatives of Firm-1 and reviewed internal Firm-1 documents and records. Based on those conversations and that review, I am aware of the following information, in substance and in part, regarding the trading operations of Firm-1:

a. A substantial portion of the trading done by Firm-1's employees is facilitated by the use of Firm-1's proprietary algorithmic trading models (collectively, the "Trading Models"). Firm-1 developed the Trading Models to, among other things, predict market movements and make trading decisions. Firm-1's employees utilize the Trading Models in making trades involving publicly traded securities and other financial products in interstate commerce.

b. A substantial portion of the trading done by Firm-1's employees is executed through the use of Firm-1's proprietary trading platforms (collectively, the "Trading Platforms"). Firm-1 developed the Trading Platforms to, among other things, create orders and automatically submit those orders to an exchange or market center, as well as execute orders. Firm-1's employees utilize the Trading Platforms in executing trades involving publicly traded securities and other financial products in interstate commerce.

c. The trading decisions resulting from Firm-1's use of the Trading Models, and the efficiencies resulting from Firm-1's use of the Trading Platforms, contribute substantially to Firm-1's market share in the financial markets in which Firm-1 trades and to Firm-1's overall trading profits. The competitive advantages and economic value that Firm-1 derives from the Trading Models and the Trading Platforms depend in part on their not being disclosed to a competitor or to the public.

d. Because of the proprietary nature of the Trading Models and the Trading Platforms, Firm-1 has put in place a variety of measures designed in part to protect the computer source code that comprises the Trading Models (the "Trading Models Source Code") and the computer source code that comprises the Trading Platforms (the "Trading Platforms Source

Code") from disclosure to a competitor or to the public. For example:

i. The Trading Platforms Source Code is maintained in a software repository platform (the "Software Repository"). Firm-1 employees use a unique login identifier and password to log into the Software Repository. Within the Software Repository, only Firm-1 employees involved in the development or support of the Trading Platforms are permitted to access the Trading Platforms Source Code.

ii. The Trading Models Source Code is also maintained in the Software Repository. Firm-1 employees use a unique encryption key to encrypt and decrypt the Trading Models Source Code. Within the Software Repository, only Firm-1 employees involved in the development of the Trading Models are permitted to access the Trading Models Source Code. Moreover, those employees are given only certain encryption keys, in order to limit their access to a subset of the Trading Models.

iii. Firm-1 does not permit its employees to utilize external e-mail or file sharing websites on their work computers. Firm-1 further does not permit its employees to download data from their work computers to USB drives or other portable storage devices.

iv. Firm-1 employees sign agreements detailing, among other things, the confidential nature of Firm-1's work and Firm-1's ownership of work product developed in the course of that work.

v. Firm-1 employees are provided an employee handbook and a code of business conduct and ethics setting forth, among other things, Firm-1's requirements that employees maintain the confidentiality of non-public Firm-1 information and protect Firm-1's proprietary information, including its trade secrets and other intellectual property. Firm-1 employees acknowledge their agreement with such policies when they are hired and periodically during their employment.

5. In the course of this investigation, I have spoken to employees and representatives of Firm-1, including, among others, technical analysts employed by Firm-1. I have also reviewed various documents, including emails and communications, provided by Firm-1. Based on those

conversations and that review, I am aware of the following information, in substance and in part, regarding the employment of ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang," the defendant, by Firm-1:

a. Beginning in or about March 2010, ZHANG was employed by Firm-1 in technical roles within Firm-1. Although ZHANG initially worked out of Firm-1's offices in the greater New York City area, in or about November 2015, Firm-1 transferred ZHANG to its offices in San Jose, California, at his request.

b. Prior to December 2016, ZHANG was assigned to the technical operations and development operations group at Firm-1, which is responsible for, among other things, ensuring that the Trading Platforms and associated trading applications function correctly, and to address any issues that might arise. While working in that capacity, ZHANG was supervised by and reported to an individual employed by Firm-1 ("Individual-1").

c. Starting in December 2016, in addition to his work for the technical operations and development operations group at Firm-1, ZHANG also began working for the infrastructure group at Firm-1, which is responsible for, among other things, systems administration and troubleshooting server, network, and hardware issues as they arise. In order to facilitate his responsibilities as part of the infrastructure group, ZHANG was granted expanded access privileges to Firm-1 computers running a Unix-based operating system, which gave ZHANG access to, among other things, the Software Repository. ZHANG was not granted expanded access privileges to other Firm-1 computers running a Windows-based operating system.

d. On or about Saturday, March 25, 2017, an individual employed by Firm-1 as a quantitative analyst ("Analyst-1") logged in remotely to Analyst-1's computer desktop on Firm-1's Windows-based network. Analyst-1 specializes in performing research and programming to create Trading Models. Shortly after remotely logging into his computer desktop, Analyst-1's remote desktop session closed because another user had logged into the same remote desktop. Analyst-1 logged in again to the remote desktop, only to see that it appeared that another user had opened the file folder that held Analyst-1's archived email mailboxes. Analyst-1 continued to work remotely through the evening but was repeatedly disconnected due to

another user logging in. Analyst-1 was able to ascertain the unique identifier associated with the other user who was logging into Analyst-1's remote desktop.

e. On or about Sunday, March 26, 2017, Analyst-1 notified Firm-1's network security group of this unusual activity, and provided the unique identifier that Analyst-1 had observed logging in to Analyst-1's remote desktop. Using that identifier, Firm-1's network security group determined that ZHANG had been accessing Analyst-1's remote desktop without authorization. Firm-1 then disconnected all computer access privileges for ZHANG.

f. Early in the morning on or about Monday, March 27, 2017, ZHANG sent an email to Individual-1, in which ZHANG wrote, in part, that ZHANG had determined that his Windows account had been terminated, which he knew "would happen because [of] what I did in the past few days and Saturday. I am still questioning myself why I did that." ZHANG further stated that on Saturday, he had "remotely logged in a few desktops randomly without authorization, using [his] Mac laptop." ZHANG explained that he was able to do so because he had modified (without authorization from Firm-1) a specific web application used by Firm-1 employees so that ZHANG could capture individual users' logins and passwords. ZHANG stated that he had done so because he was aware of a potential acquisition of Firm-1, which he believed might place his job at risk, and that he sought to understand the status of the company through gaining access to these users' accounts.

g. Later that day, ZHANG sent a text message to Individual-1, stating in part that he was about to go to the office "to hear [the] verdict" and asking if Individual-1 was available to speak. Individual-1 and ZHANG then had a telephone conversation, in which ZHANG admitted to Individual-1 that he had also accessed the remote desktop of another quantitative analyst based in Firm-1's headquarters in New York City ("Analyst-2").

6. In the course of this investigation, I have spoken to employees and representatives of Firm-1, including, among others, technical analysts employed by Firm-1. Based on those conversations, I am aware of the following information, in substance and in part, regarding Firm-1's subsequent broader

investigation of the activities of ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang," the defendant:

a. In the course of its investigation of ZHANG, Firm-1 has reviewed various data relating to ZHANG's computer activity. Pursuant to that review, Firm-1 has found evidence that ZHANG successfully exfiltrated the source code for multiple Trading Models and Trading Platforms to a third-party software development site (the "Development Website"). Firm-1 has found evidence that ZHANG's efforts to steal this data began at least as early as December 2016.

b. Firm-1's technical staff determined that ZHANG installed on Firm-1's systems computer code designed to look for encryption keys on the servers used to build the Trading Models. Doing so would have enabled ZHANG to gain access to much larger portions, if not the entirety, of the Trading Models Source Code.

c. In addition, Firm-1 identified an area of its computer networks where ZHANG stored data - over 3 million files - prior to uploading it onto the Development Website. Firm-1's review of that data shows, among other things, that ZHANG gained unauthorized access to unencrypted portions of the Trading Models Source Code.

d. In addition, Firm-1 identified computer code that ZHANG had written to exfiltrate data to the Development Website. Firm-1's review of that data shows, among other things, that ZHANG uploaded to the Development Website unencrypted portions of the Trading Models Source Code, as well as email mailbox files assigned to the head of the quantitative side of Firm-1's market making group. ZHANG also accessed the Development Website thousands of times from Firm-1's networks.

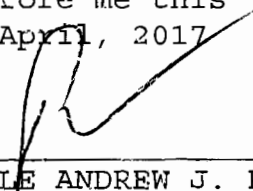
e. All communications between Firm-1's computer network and the external internet pass through a proxy server. Firm-1's primary proxy server is maintained by a third-party vendor. Firm-1's backup proxy server is maintained at Firm-1's data center in Purchase, New York. The computer code that ZHANG wrote to exfiltrate data to the Development Website was designed to route all of the data through Firm-1's backup proxy server in Purchase, New York.

WHEREFORE, I respectfully request that an arrest warrant be issued for ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang," the defendant, and that ZHANG be arrested and imprisoned or bailed, as the case may be.



MICHAEL DENICOLA
Special Agent
Federal Bureau of Investigation

Sworn to before me this
3rd day of April, 2017



THE HONORABLE ANDREW J. PECK
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK